Communications Architecture Recommendations to Enable Joint Vision 2020

Track 8 – Space C2 Applications

LCDR R. Bronson Armstrong, USN
National Security Space Architect
11242 Waples Mill Road
Fairfax, VA 22030
571-432-1389
robert.armstrong@osd.mil

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **JUN 2003**	2. REPORT TYPE	3. DATES COVERED **00-00-2003 to 00-00-2003**
4. TITLE AND SUBTITLE **Communications Architecture Recommendations to Enable Joint Vision 2020**		5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Security Space ,11242 Waples Mill Road,Fairfax,VA,22030**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**12**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Abstract

The Mission Information Management (MIM) Communications Architecture provides a framework to develop an integrated space, air, and terrestrial communications network that supports all national security users (DoD, Intelligence Community, and civil), all information domains, and all levels of classification. The architecture provides a basis for developing a communications investment strategy to satisfy Joint Vision 2020 imperatives. The architecture framework consists of an integrated, internetted high capacity space backbone, high capacity terrestrial gateways, fiber entry points, airborne communications nodes, and software programmable tactical terminals that are handheld or embedded on weapons platforms. Dynamic routing, prioritization, and bandwidth allocation in space, air, and terrestrial layers ties the architecture together, eliminates stovepipes. An NSSA led Architecture Development Team comprised of thirty stakeholder organizations developed the architecture and a set of proposed recommendations for presentation to the NSSA Senior Steering Group.

The Mission Information Management Communications Architecture

On 7 December 1998, the NSSA Senior Steering Group(SSG), comprised of Arthur Money (Assistant Secretary of Defense for C3I), Joan Dempsey (Deputy Director for Central Intelligence Community Management) and Lt Gen Frank Campbell (Joint Staff J8), directed the National Security Space Architect to "develop and architecture and investment strategy recommendations to guide acquisition planning and program execution for National Security mission information management (MIM) capabilities in the 2010-2025 era. MIM comprises all aspects of providing mission essential information to mission executing entities-DoD, intelligence, and civil." The NSSA was subsequently tasked by the SSG to develop an overarching communications architecture that includes space, air, and terrestrial layers. The NSSA MIM Communications Architecture (CA) team led a collaborative Architecture Development Team (ADT) that consisted of 30 stakeholder organizations from throughout the DoD, the intelligence community (IC), and the National Aeronautics and Space Administration (NASA). The initial ADT meeting took place in July 2000. The ADT completed the development of the communications architecture and proposed recommendations in April 2001.

JV 2020 Imperatives

JV 2020 states that combat forces must close in theater rapidly, conduct decisive operations immediately after closing, be highly agile in order to shift combat power form one objective to another at will. JV2020 also states that combat forces must fight in non-linear enclaves in which joint forces converge and focus combat power at relatively low tactical levels. Traditional service boundaries will be blurred or eliminated. Forces must achieve information dominance. This implies that warfighters at all levels must have immediate and uninterrupted access to all relevant information regarding friendly and enemy situational awareness, future plans, and operational status. This information may be located in national databases in CONUS, in CINC databases in secure sanctuaries outside of CONUS, or in operational and tactical level databases in Joint Task Force areas of operations.

Recommendations

The CA ADT investment strategy recommendations address communications as an enterprise They describe a set of integrated space, air, terrestrial, and network communications elements that must be implemented to treat communications as an enterprise.

Goal: Treat Communications as an Enterprise

Currently, communications are treated in an *ad hoc* basis by individual organizations, agencies, services, and their subdivisions. This approach means that any opportunity for synergy and interoperability is serendipitous, at best, and costly and inadequate, at worst. By treating communications as an enterprise, in the business sense, end-to-end and government-wide, there is the opportunity to maximize communications performance and reduce costs by allocating resources and functionality rationally across terrestrial, air, and space layers. In addition, there is the further opportunity to increase efficiency by allocating within the space, air, and terrestrial layers across organizations.

Why treat comms as an Enterprise?

- Enables trades among all elements
- Promotes interoperability
- Reduces overlap / unnecessary duplication
- Promotes enterprise-wide efficiency
- Best matches limited assets to needs
- Maximizes performance and reduces costs

Overarching Recommendation: Integrated, robust network over the space, air, and terrestrial environments with dynamic routing, prioritization, and bandwidth allocation:

Many major national security networks, especially the long-haul space networks, are currently circuit switched. While circuit switching is a powerful technique that is appropriate for many types of service, there are some services that are better suited to other techniques such as packet switching. Therefore, the NSSA recommends upgrading the capability of networks over all communications layers, space, air, and terrestrial to make them better suited to bursty traffic to provide more efficient exchanges of data between multiple users and multiple types of users.

The reason for this networking approach is to improve interoperability among systems and provide tools to support the effective management of limited communications resources within the National Security Community.

The networking domain relies almost exclusively on the use of commercial standards, protocols, and applications to achieve interoperability. Implementing packetized networks is a low technical risk venture because of the maturity of the technology and vendor acceptance of the associated standards. The ADT agreed in principle that a movement toward a packetized network environment would be a major enabler for achieving interoperability. However, military network standards may require integration with the commercial networks. Hybrid networking may be necessary to accommodate military-unique features.

A mobile, *ad hoc*, self-organizing networking capability is needed to support rapid deployment forces and reduce the burden on strategic lift.

"*A mobile ad hoc network (MANET) is an autonomous system of mobile routers (and associated hosts) connected by wireless links. . . . The routers are free to move randomly and organize themselves arbitrarily…*"[1]

[1] *MANET Working Group Charter, Internet Engineering Task Force*

Reconfigurable Wireless Networks (RWN), a sub-group of MANET, allows several nodes, a large network span, and a wide range of network mobility. MANET RWNs can be rapidly deployed without relying upon organic or existing terrestrial infrastructure. The Services need to minimize strategic lift requirements for combat support systems, and an *ad hoc* reconfigurable networking capability would provide for this operational need. Bandwidth and spectrum are not unlimited. Packetized networks in concert with automated network management tools are needed to effectively manage these limited resources.

Primary Recommendations

The CA ADT recommended the following primary capabilities to achieve the goal of a communications enterprise:

- Terrestrial Optical Networks
- Airborne Communications Nodes
- Interoperable Space Crosslinks
- Multi-Mode, Multi-Band Terminals

- Enables IM architectures
- Leverages commercial trends
- Enables interoperability per vision statements
- Increases network efficiency for bursty[1] traffic
- Is required for multi level

Terrestrial Optical Networks - All fixed users should use fiber as primary communications

The evolution of global communications in the commercial sector has significantly outpaced military technology for requirements in which economic initiatives have been favorable. Fiber-optic cable is being laid at ever-increasing rates. Where capacity is available and vulnerability is acceptable, integrating commercial resources with government systems ease the burden on dedicated government systems. Government-developed systems should therefore focus on mission-unique requirements for coverage, survivability, and dictated requirements outside the commercially feasible market. Commercial resources need to be integrated in instances where the providers can ensure high volume, fixed locations, low latency, low risk of loss of service, and access. The ADT recommended the following action:

- Communication service between fixed users should migrate toward cost-effective commercial resources, including terrestrial optical networks and/or space consistent with operational requirements. DoD communication programs should focus on requirements (coverage, security, survivability, and dynamic change) not satisfied by commercial services.

The implementation of this recommendation will reduce costs by relying on installed fiber where feasible and be a step towards treating communications as an enterprise. The installation of new fiber should proceed where appropriate to offload from space communications while retaining the option for wide-band satellite backup.

Why Terrestrial Optical Networks?

- Enables IM Vision
- Provides fixed users with most cost-effective service
- Bandwidth unconstrained by spectrum availability
- Can be as secure as space transmissions
- Low latency
- Let costs across the enterprise drive implementation

Airborne Communications Node To Augment Ground Infrastructure – Develop a robust agile network that delpoys a mobile force

The ADT recommended the development of Airborne Communications Nodes (ACNs) for three primary reasons:

- *Enables the last tactical mile*
- *Enables the future user class envisioned to need wide-band two-way communications to highly mobile small terminals*
- *Moves most maneuver ground communications infrastructure to high altitude to solve mobility, capacity and ground threat problems.*

Current terrestrial communications networks are not as mobile as their supported maneuver elements. The ability of these networks to support highly mobile forces and small, dispersed units on a non-linear battlefield is marginal.

A deployable ACN could support a strategically responsive force enabling dominance across the full spectrum of operations. This concept significantly reduces strategic lift and supports highly mobile decisive military operations. It reduces the extensive manpower, equipment, and associated ground forces currently required for tactical communications. This in turn reduces the requirements for personnel end strength and support equipment associated with ground communications. ACNs can self-deploy and thus enable the Army goal of deploying five divisions in 30 days. ACNs extend the range of ground radio nets. They provide a highly responsive network blanket for mobile forces and bridge the gap between satellite coverage and terrestrial fiber.

The candidate for the ACN used for CONOPS and costing by the ADT is the current Global Hawk platform. The team was particularly concerned about two issues with ACNs:

- There is no funding for development of a production Global Hawk communications platform
- Engineering work has yet to be done for integrating optical heads on a Global Hawk platform to provide high-capacity uplinks to the Space Domain.

Commercial platforms were considered and closely examined in this study. They are reaching a level of maturity that will allow them to support enduring missions that do not require rapid deployment and quick strike operations. They can augment Government ACNs.

The ADT recommended the following actions to ensure the development of a robust agile network that deploys quickly and supports a highly mobile force:

- *Develop airborne communications node to enable Joint Vision 2020 imperatives that rely upon reachback communications, reduced strategic lift, and early and rapid closure of the last tactical mile especially to handheld terminals and mobile platforms.*
- *Develop cross-linked airborne communications nodes to provide air-to-space, space-to-air, air-to-ground, and ground-to-air connectivity to include teleports and fiber-head gateway connections. Future communications satellites must include adequate connectivity to these ACNs. Appoint an executive agent to develop this critically needed capability.*

Why ACNs?

- Enables wide-band "On the Move" to hand held terminals (HHTs)
- Multiplies the number of simultaneous users (freq reuse)
- Moves Most Maneuver Ground Communications Infrastructure to ~ 65kft to Solve Mobility, Capacity Problems
- Enhances theater-wide wide-band reachback
- Enables new strategies
- Rapidly deployable; reduces strategic lift requirements
- Reduces unit cost & complexity of terminals

Interoperable Space Crosslinks – Improve Space Segment Capabilities and support to National Security Systems

The ADT recommended the following actions to improve space capabilities and support to national security systems, and as an essential step in the development of a space network:

- *Acquire common interoperable cross-linked space communications satellite constellations to improve reachback, network performance, interoperability, survivability, and support to disadvantaged users. Initially, these links might be used only as intra-constellation links.*

- *Establish common radio frequency (RF) and optical standards for the communications and relay satellite cross-links so that cross-constellation and common connections will support the migration to an integrated relay-backbone system as required at a future date.*

.

The initial advantages of the interoperable cross-link architecture are that it:

- *Increases survivability and user up/downlink capacity*

- *Reduces reliance on teleports*

- *Provides total coverage from CONUS ground stations. OCONUS ground stations can provide alternative backup.*

Why Interoperable Space Crosslinks?

- Increases survivability
- Increases Mission Adaptability
- Essential for network vision
- Reduces overall costs
- Reduces dependence on ground stations
- Allows DoD / NASA to leverage off IC technology advances
- Reduces latency

Multi-Mode, Multi-Band Terminals – Continue and accelerate the Joint Terminal Engineering Office (JTEO) Roadmap

Terminals represent a large cost (50 percent of end-to-end systems cost by some estimates) and a large impediment to rapid change due to high installation costs and lead times. Furthermore, the number of terminals an individual user may require (for radio, LAN, UHF, SHF, and EHF connectivity) becomes burdensome. The commercial sector has solved this problem by offering multi-mode, multi-band radios, cell phones, and so on. The current trend is to encode the mode in software or firmware, making the addition of new formats and waveforms is simple as replacing a PMCA card or loading a new application. The ADT recommended that this migration be continued and expanded. For instance, the current Joint Tactical Radio System (JTRS), while a reasonable start, needs to be expanded to frequencies above 2 GHz along the lines of the Multiple Integrated Smart Terminal (MIST) program. These terminals must include a packet ready capability as demonstrated by the 8-band, programmable, networked terminal test beds at the Naval Research Laboratory.

The implementation of this recommendation will provide the following benefits:

- *Reduces burden on user*
- *Improves interoperability across the enterprise*
- *Provides packet ready terminals for all users*
- *Facilitates future upgrades through software programmability*
- *Includes hand-held through "ground station" size.*

The Joint Terminal Engineering Office (JTEO) reports that efforts to implement this recommendation are on track, but the ADT believes that the efforts must be accelerated, especially for high capacity hand-held terminals.

Why Multi-Mode, Multi-Band Terminals?

- Promotes interoperability
- Promotes mission adaptability
- Eases transition
- Lower total cost

Supporting Recommendations

The following supporting recommendations enable or enhance implementation of the primary recommendations:

- Multi-User Single Government Relay System with High-Capacity Ground Terminals
- Cross-Banding
- Research and Development
- Future Traffic Projections Model / Modeling and Simulation
- Information Assurance / Security

Multi-User Integrated Government Relay System with High-Capacity Ground Terminals – Combine currently separate relay functions

The CA ADT recommended the following actions to integrate the government and commercial terrestrial, space, and airborne communications:

- *Combine the primary functions of the NRO and NASA relays into a single cross-linked satellite system and consolidate ground stations with both packet and circuit-switching capabilities*
- *Develop multi-gigabit capacity ground terminals to integrate space and airborne assets into the terrestrial fiber network.*

The implementation of this recommendation

- *Potentially reduces costs through NRO/NASA infrastructure simplification*
- *Consolidates most national security relay functions on one cross-linked relay constellation*
- *Provides multi-gigabit connection for the space network to the terrestrial network which is an improvement over current capacity*
- *Gives expanded opportunities for other relay use*
  - *En route communications*
  - *Presidential communications*
  - *Wideband aircraft*
  - *NPOESS satellites*

Why combine relay functions with high-capacity ground terminals?

- Potential to Reduce cost by reducing infrastructure
- Supports expanded set of users
- Expands capacity for all users

Cross-banding – Rapidly and automatically Connects All Users

Cross-banding is the ability for the information flow on different "bands" (UHF, SHF, EHF, commercial, relay, terrestrial, airborne, and so on) to be interconnected. While this is not always possible (wideband traffic cannot successfully flow over narrowband communications systems), there is a broad need for as much cross-banding as possible. Recommend that all packet switches be implemented with cross-banding capabilities, and the "smart delivery" provision of the Information Management architecture be used, together with user profiles, to inhibit cross-banding where it doesn't make sense. The implementation of this recommendation will enable all National Security Satellite Communications (Relay, Wideband, Narrowband, and Protected) to create a unified network. The implementation will also enable the space, airborne, and terrestrial components to work as one cohesive enterprise. The packetization of the National Security Communications Networks is a prime enabler to the realization of this recommendation.

Why cross-banding?

- Provides Total Interconnectivity
- Enables Future Visions
- Enhances Interoperability
- Enhances Mission Adaptability

Supporting Research and Developmen – Leveraging evolving commercial trends and invest government R&D dollars only where requiredt

Commerce has displaced the government as the main engine for developing advanced information technology and innovative approaches for delivering information. While these advances and innovations may satisfy some critical National Security Community needs, they are generally brought to market only if there is a credible business case to justify the investment. Because some needs are unique to national security, the National Security Community must take on a portion of the burden of system development. This path, however, negates the advantages of commercial economies of scale found in production and associated costs.

The U.S. Government invests approximately $4.5 billion (FY00) to acquire, operate, and maintain its national communications architecture. In addition, approximately $1 billion (FY00) was invested in basic science and research for communications and information management

technologies. To fully develop the national security communications capabilities described in this report, the distribution of R&D funds should include the following proposed research activities.

- *Continually assess the basic commercial research and evolving products with the potential to support implementation of the MIM architecture.*
- *Perform research and development to acquire military-unique capabilities.*
- *Perform research and development to integrate mission specific network data into common packetized networks.*
- *Provide funding to support mission enabling technology initiatives:*
  - Laser communications technology (Commercial Leverage)
  - Long loiter Airborne Communications platforms (Commercial Leverage)
  - Airborne communications packages (Commercial Leverage)
  - High bit-rate protocols for high latency earth-satellite links
  - Multi-Mode, Multi-Band handheld, packetized terminals (Some Commercial Leverage)
  - High rate, software programmable packet switching (Commercial Leverage)
  - High speed encryption
  - High capacity ground terminals (bandwidth efficient modulation for multi gigabit up/down links)

- Network management tools including congestion detection and mitigation (Some Commercial Leverage)
- Dynamic networking (*ad hoc*, self organizing, self healing)

Why?
- ♦ Saves scarce resources

Consolidated Traffic Models & Modeling and Simulation Capabilities – Gather message statistics to develop realistic traffic models

The ADT recommended the national security communications components develop traffic models to support system development and planning and course-of-action analysis. This development can be accomplished by continuously monitoring consolidated enterprise-wide traffic through instrumentation and analysis. The models then can project future traffic resulting from improved strategies and tactics and evolving missions. DoD and IC traffic models and information exchange requirements should be developed from the NCA through the theater to the interface with the joint force supporting and supported components. A pilot project to determine scope and resources needed to develop a full-scale traffic model could be useful.

Once reasonable traffic models are developed, modeling and simulation tools will need to be developed to allow for the presentation of network situation awareness in real-time and assess policy implications on network efficiency in near real-time. The National Security Community needs a capability for real-time situation awareness analysis and near real-time planning, communications policy assessments, and course of action analysis. Commercial enterprises provide some analysis and timeliness capabilities. While commercial tools should be used as much as possible, some R&D investment is necessary to add message prioritization and other unique requirements.

The ADT recommended the development of:

- ♦ *Projected future communication needs over entire enterprise in terms of message size, usage profile, and type*
- ♦ *Enterprise-wide network modeling and simulation tools*

The combination of these elements will allow the following:

- ♦ *Element and enterprise trades based on realistic performance estimates*
- ♦ *Real-time, efficient network control*

Why traffic models?
- ♦ Allows communication system designs to be optimized
- ♦ Enables real-time network management
- ♦ Emerging Requirements Database (ERDB) database is inadequate for network centric architecture

Information Assurance / Security – Develop a robust enterprise wide information assurance architecture

Information Assurance (IA): Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. *(DODD S-3600)*

The ADT did not address the Information Assurance (IA) function during the development of the point designs and recommendations primarily because other elements of the GIG enterprise were actively addressing IA issues and because of time and resource constraints. A basic need is for real-time visibility into and network security monitoring of system user, local area, and wide area network traffic profiles and volume. These capabilities, along with other measures such as link encryption and tunneling of addresses, are vital for network managers and operators to detect, protect, and recover the computer and communications infrastructure from malicious re-routing, spoofing, and denial-of-service attacks. The team recognized the need for a National Security Community strategy to implement such a capability.

Few business enterprises require protection to the same level as national security communications systems. The global banking and finance community, however, has a similar requirement to protect sensitive information. If the protection measures acquired by this community satisfy some of the national security communications needs, then those measures should be applied. Because of the sensitivity and classification of national security information, the community should not fully rely on the commercial market to develop the capability. A business case may not exist for the commercial world to lead the way in the national security IA domain.

Network Security Monitor (NSM) products and standards are available on the open market. However, the integration of the NSM with other needed network management and simulation tools suitable for the real-time national security environment must be addressed.

Tunneling of addresses is a useful firewall technique to disguise addresses for protection against network spoofing, or misrouting.[2] Protection against network spoofing requires limiting access to network switches and Network Security Monitor (NSMs) as well as the use of strong authentication mechanisms. Such mechanisms exist and are not viewed as a developmental requirement, although incorporation of such protection is an essential component of the MIM architecture.

The ADT recommended the following actions to achieve some limited measure of information assurance:

- *Develop an information assurance architecture, including optical security, to enable implementation of the national security MIM recommendations.*

[2]Network spoofing as discussed in this document is limited to the misdirection of traffic typically caused by access to the network routing tables and NSMs.

- *Develop a multi-gigabit (greater than 2.5 Gb/s) encryption capability for use over packetized networks and connections.*

- *Specify traffic flow security approach for the MIM architecture to provide the following:*
  - Availability
  - Integrity
  - Authentication
  - Confidentiality
  - Non-repudiation.

Why?

- Protect against external computer network attacks
- Protect against insider threat
- Enable either MLS/MSL architecture (details in appendix)
- Supports IM's user profile

National Security Space Architect
Mission Information Management
Communications Architecture Team Members

LCDR Robert B. Armstrong	NSSA
Lt Col Peter R. Axup	NSSA
Dr. John C. Baker	CSC
Maj Catherine A. Baum	NSSA
Jennifer A. Buchanan	ASI
Gene T. Collingsworth	FTI
Hoyt A. Cruz	SAIC
Dr. Michael P. Healy	AEROSPACE
Maj Roger H. Hill	NSSA
Dennis L. Hippensteel	NSSA
Bruce G. Jackson	MITRE
Thomas J. Kacena	AUTOMETRIC
James T. Kindle	NRO
James L. Kingston	MITRE
Janice Singleton-Vincent	AUTOMETRIC
Patricia Tiernan-Waugh	AUTOMETRIC
Thomas J. VanHorn	TECELOTE